

## **Adware**

Software that displays advertising content on your computer. Like its cousin spyware, some adware runs with your full knowledge and consent, some do not. More often an annoyance than a security risk, adware may also monitor browsing activities and relay that information to someone else over the Internet.

## **Asymmetric encryption**

An encryption method using a widely published public key to encrypt messages, and a corresponding private key to decrypt them.

## **Backup**

An extra copy of computer files, usually kept physically separate from the originals. Essential for recovery when original files are damaged or lost.

## **Blended Threat**

An attack combining a number of traditional attack methods, like a worm, a Trojan horse, and a keylogger. Most require a combination of security tools and protection layers to defend.

## **Blog**

Derived from Web log: Web site where an individual displays journal entries or commentary on a regular basis. Some blog owners allow others to post entries on their site.

## **Bluetooth or IEEE 802.15.1**

Named after 10th century Danish King, Harald Blatan (Bluetooth), who was known as a uniter: a conventional set of wireless standards for short-range communication between wireless headsets, phones, PDAs, keyboards, and other disparate devices. Bluetooth supports a number of security measures, but it had flaws that could expose Bluetooth-enabled devices to attack.

## **BOT or Web BOT**

Derived from robot: an automated program, such as a Web crawler, that performs or simulates human actions on the Internet. Used for legitimate purposes by search engines, instant message (IM) programs, and other Internet services. Can also be used to take control of computers, launch attacks, and compromise data; may act as part of a blended threat. See also, Botnet.

## **Botnet or zombie armies**

A group of computers which have been compromised and brought under the control of an individual; the individual uses malware installed on the compromised computers to launch denial-of-service attacks, send spam, or perpetrate other malicious acts.

## **Certificate authority**

In public key cryptography, a trusted third party who authenticates entities and their public keys. To do so, certificate authorities issue digital certificates, which validate that a public key belongs to the person whose digital signature is listed on the certificate.

## **Chat room**

An online forum where groups can exchange comments in real time. Many chat rooms use moderators to monitor behavior and control access. However, chat room users can join anonymously, and sexual predators have used that anonymity to disguise themselves and target unsuspecting children and teens.

## **Cookie**

A small text file placed on your computer when you visit a Web page. Used to remember you and your preferences when you revisit that page or to track your browsing activities, cookies facilitate virtual shopping carts, page customization, and targeted advertising. They are not programs and cannot read your hard drive or cause damage to your computer.

## **Defragment or Defragging**

Process of reorganizing information on your hard drive by placing parts of files in a more logical order and in closer proximity to one another. Fragmentation can slow down your computer; when defragmented, drives are faster and have larger areas of free space.

## **Digital certificate**

Also called public key certificate or identity certificate: In public key cryptography, validates that a public key is owned by the entity sending encrypted or digitally signed data with that key. Digital certificates are issued by a certificate authority and contain the sender's public key plus a digital signature verifying that the certificate is authentic and that the key belongs to the sender.

## **Digital signature**

Used in public key cryptography to validate the integrity of encrypted data and to confirm both the identity of a digital certificate holder and the authenticity of the certificate itself.

## **Domain spoofing or Domain hijacking**

Manipulation of the domain name system to associate a legitimate Web address with an imposter or otherwise malicious Web site. Used to perpetrate phishing and other types of attack, the user is sent to the imposter Web site with little or no warning.

## **DoS**

Denial-of-Service: an attack on a computer or network in which bandwidth is flooded or resources are overloaded to the point where the computer or network's services are unavailable to clients. Can also be carried out by malicious code that simply shuts down resources.

## **Encryption**

A security method that makes information unreadable to anyone who does not have a key to decipher it; commonly used to secure online purchases and other transactions. When a Web site indicates it's "secure" that usually means the data you send and receive is encrypted. See also, public key cryptography.

## **File**

Compression or Data compression – Reducing a file’s size by encoding its contents. Compression is used to maximize storage space and to facilitate faster transmission over the Internet. Compressed files are often placed in an archive file and must be extracted and decompressed before use; others are used in a compressed state. Common compression archive formats include .ZIP, .SIT, .TAR, .JAR, and .CAB. See also, image compression.

## **Firewall (network)**

A hardware or software device - or both, that controls network access and communications between a network and the Internet, or between one part of a network and another.

## **Firewall (personal)**

Software that controls access and communications between a computer and the Internet or a local network. Blocks hackers and other unauthorized traffic, while allowing authorized traffic through.

## **FTP**

File Transfer Protocol: a conventional set of communication rules for transferring files between computers on the Internet. While most Web browsers can transfer files using FTP, you can also use a dedicated FTP program, which usually provides better security features.

## **GIF**

Graphics Interchange Format: an image file format popular on the Internet. GIFs are favored for graphics because they can be compressed without losing image quality. However, GIFs are limited to 256 colors and are therefore unsuitable for digital photos. See also, JPEG.

## **Hacker**

Commonly, a person who uses programming skills and technical knowledge to gain unauthorized access to computer systems for malicious or criminal purposes. The programming community, however, prefers to use the term cracker for such persons; they reserve hacker for any well-respected, highly skilled programmer.

## **HTML**

Hypertext Markup Language: the principal language used to create and format Web pages. Controls the layout, design, and display of text, hyperlinks, images, and other media on most Web pages.

## **HTML tags**

The standard set of HTML code elements used to create and format Web pages.

## **HTTP**

Hypertext Transfer Protocol: a conventional set of communication rules for controlling how Web browsers and servers pass information back and forth over the Internet.

## **HTTPS**

HTTP conventions for passing information to a server that is secured using encryption and/or authentication measures. The URL of Web sites offering secure HTTP connections begin with https://.

## **Hyperlink**

A clickable word, phrase, or image that takes you from one Web page to another Web page or resource on the Internet. Hyperlinks are created using HTML tags, and when displayed in a browser, they are typically underlined or set apart by a different color.

## **IM**

Instant Message/ Messenger: Programs that allows two or more people to communicate with one another over the Internet in real time. While most IM communications occur as text, some IM programs also offer streaming audio-visual conferencing and file exchange services. IM can also refer to messages sent by instant messaging, or to the act of sending an instant message.

## **Image Compression**

Image compression: Reducing the size of an image file, while maintaining an acceptable level of quality. Used extensively on the Web, JPEG and GIF are common compressed image file formats. Also see file compression.

## **Internet or the Net**

A public, worldwide network of computers and computer networks. The World Wide Web, email, instant messaging, chat rooms, and many other online services and data transmissions are facilitated by the Internet.

## **IP Address**

Internet Protocol address: a unique identifier for each computer or other device on a network, including the Internet. Conceptually similar to a phone number, IP addresses are a string of numbers that allow computers, routers, printers, and other devices to recognize [identify] one another and communicate.

## **JPEG**

Joint Photographic Experts Group: a popular compressed file format for digital photos. JPEGs are favored on the Web because they can be compressed while maintaining high resolution; many digital cameras create JPEGs by default. The file extension for JPEGs is .jpg or .jpeg. See also, GIF.

## **Keylogger**

Software that monitors and captures everything a user types into a computer keyboard. Used for technical support and surveillance purposes; can also be integrated into malware and used to gather passwords, user names, and other private information.

## **mp3**

MPEG Audio Layer 3: a compressed audio file format, popular for playing sound and music recordings over handheld and desktop audio players.

## **Malware**

Derived from malicious software: software designed to do harm by causing damage to systems or data, invading privacy, stealing information, or infiltrating computers without permission; includes viruses, worms, Trojan horses, and some keyloggers, spyware, adware, and bots.

## **Mutual authentication**

A security method requiring both parties to a transaction to prove their identities. On the Web, this would require both the Web browser and Web server to prove their identities to one another, thus ensuring both the Web page and the page's user are legitimate. Used on financial and commerce sites, mutual authentication can help prevent phishing and other kinds of fraud.

## **Network or Computer network**

A group of two or more computers connected by cables or wireless signals or both, which can communicate with one another using network protocols. Networks can also include other devices, including printers, routers, and network hubs.

## **Network hub**

A hardware device that connects computers to one another on a local network.

## **PDA**

Personal Digital Assistant: a handheld computer usually containing address books, memo pads, and other personal organization software. Many PDAs can connect to the Web, send email, and synchronize with home computers; some work as cellular phones.

## **Phishing**

An attempt to mislead people into divulging confidential information, such as social security numbers and passwords. Typically uses legitimate-looking email or IMs in combination with imposter Web sites to make fraudulent requests for information (i.e., to go "fishing" for data). See also, social engineering.

## **Pharming**

An attempt to defraud Internet surfers by hijacking a Web site's domain name, or URL, and redirecting users to an imposter Web site where fraudulent requests for information are made. See also, URL spoofing.

## **Podcast**

Derived from iPod and broadcasting: a regularly updated set of mp3 audio files available on the Web for one-time download or subscription. Podcast subscribers receive updates automatically via RSS Web feeds.

## **Private Key**

In asymmetric encryption, an unpublished key used to decrypt messages encrypted using a corresponding public key.

## **Public key**

In asymmetric encryption, a key made available to anyone who wants to send an encrypted message to the owner of the key. The owner of the public key uses his or her private key to decrypt messages.

## **Public key cryptography**

An encryption technique using public keys to encrypt messages, digital signatures to validate the integrity of messages, and digital certificates to authenticate the identity of public key owners.

## **Public key infrastructure or PKI**

A set of standards and services designed to support public key cryptography. Uses digital certificates issued by certificate authorities to authenticate public keys and the entities who own them.

## **Recovery**

The process of using backups to restore original data files that have been damaged or are no longer accessible.

## **Router**

A hardware device that connects two networks and directs traffic from one network to the appropriate destination on the other. Often used to connect a network to the Internet, some routers have network firewalls and other features built into them.

## **RSS**

Really Simple Syndication: an XML format used to create Web feeds of content available on news sites, blogs, and other Web sites with fast-changing information. The feeds generally contain headlines and summaries of content and subscribers use RSS readers to view them.

## **Symmetric encryption**

An encryption method using the same secret key to encrypt and decrypt messages.

## **SMTP**

Simple Mail Transfer Protocol: a conventional set of communication rules for sending email messages over the Internet.

## **Social Engineering**

A method of deceiving users into divulging private information, social engineering takes advantage of our natural tendency to trust one another rather than relying solely on technological means to steal information. Often associated with phishing, pharming, spam, and other Internet-based scams.

## **Spam**

Unsolicited email, usually sent in bulk to a large number of random accounts; often contain ads for products or services. Also used in phishing scams and other online fraud. Can be minimized using email filtering software.

## **SPIM or Instant spam**

Unsolicited instant messages, usually sent in bulk to a large number of IM accounts; often contain marketing materials and links to product Web pages. May also be used in phishing scams or to spread malware. See also, spam.

## **Spit**

Spam over Internet telephony; unsolicited VoIP phone calls sent in bulk over the Internet. Not yet a major annoyance or threat, but could become a serious problem as VoIP becomes more popular. Also, see Spam and SPIM.

## **Spyware**

Software that collects information about your computer and how you use it and relays that information to someone else over the Internet. Spyware ordinarily runs in the background and in some cases installs itself on your computer without your knowledge or permission.

## **Trojan Horse**

A malicious program disguised as legitimate software; often gives someone else the power to take remote control of your computer; may also attack data or systems. Unlike viruses and worms, Trojan horses cannot replicate or propagate themselves and therefore must rely on other methods of distribution.

## **URL**

Uniform Resource Locator: a Web site or Web page's address (e.g., [www.symantec.com](http://www.symantec.com) or [www.symantec.com/home\\_homeoffice/index.html](http://www.symantec.com/home_homeoffice/index.html)). Browsers use URLs to identify and download Web pages from the Web servers where they are located.

## **URL spoofing**

Attempting to masquerade or closely mimic the URL displayed in a Web browser's address bar. Used in phishing attacks and other online scams to make an imposter Web site appear legitimate; the attacker obscures the actual URL by overlaying a legitimate looking address or by using a similarly spelled URL.

## **Virus**

A program that can self-replicate and infect files, programs, and computer systems; some viruses simply replicate and spread themselves, while others can also damage your computer system and data.

## **VoIP**

Voice over Internet Protocol; digital telephone service that facilitates voice transmissions over the Internet or other IP networks.

## **Wardriving**

Derived from wardialing, a similar, modem-based technique made popular in the movie *WarGames*: driving the streets with Wi-Fi enabled devices to detect open or unsecured wireless networks. Some wardrivers use GPS devices to map and then publish the whereabouts of the networks they find.

## **Warchalking**

Derived from wardriving: drawing symbols in public places to indicate the location of open or unsecured wireless networks.

## **Web or the World Wide Web**

An information sharing service running on the Internet, the Web is a worldwide collection of computers, or Web servers, which make Web pages and other files available to the public. Web browsers use URLs to identify Web pages and files, and they make HTTP or FTP requests to retrieve them. Most Web pages contain hyperlinks to other pages or files; thus the term Web.

## **Web browser**

A program used to download, display, and navigate among Web pages. Web browsers primarily use HTTP to communicate, and they can display a variety of files types, including HTML, XML, JPEG, GIF, and MPEG. Most browsers can run small programs written in Java, ActiveX, and JavaScript, and many can encrypt transmissions for security purposes.

## **Web crawler or spider**

A BOT that methodically browses the Web. Used by search engines to automatically download a vast number of Web sites, which are then indexed to make searches more efficient. Can also be used to do Web site maintenance or to harvest email addresses for spam purposes.

## **Web feed**

A file, usually in XML format, containing headlines and summaries of fast-changing Web content, like news stories, podcasts, and blogs. Web feeds provide links to full versions of content for subscription or one-time download; they can also be shared and republished by other Web sites, creating a sort of online syndication. See also, RSS.

## **Web page**

A file, usually in HTML format, available for retrieval by a browser on the Web. Web pages can contain text, images, and multi-media resources. They usually include hyperlinks to other Web pages or files, and some contain forms through which you can send information to the page host.

## **Web server**

A computer that makes Web pages and other resources available for sharing over the Internet. Using HTTP, Web browsers request pages from Web servers, which then send, or download, those pages to the requester. Also refers to a program that facilitates a Web server's functions.

## **WEP**

Wired Equivalent Privacy: part of the 802.11 IEEE standards, WEP is a security protocol for encrypting information and preventing unauthorized access to wireless networks. Designed to provide as much security as hard-wired networks, WEP has serious flaws and has been replaced by WPA and WPA2 as the preferred wireless security protocols.

## **Widget**

Generally an interactive graphic component, like a button, check box, window, or text box. Also refers to small, desktop programs like Apple's Dashboard components and Yahoo! Widgets, which display real-time information and provide quick access to commonly used functions.

## **Wi-Fi**

Wireless fidelity, a play on the term hi-fidelity: descriptive term used to refer to 802.11 wireless networks, devices, or anything associated with 802.11 wireless technology (e.g., Wi-Fi hotspot).

## **Wi-Fi hotspot**

A physical area where you can use a Wi-Fi-enabled device to connect to the Internet over a public wireless network. Some hotspots have no security measures in place, while others use WEP or WPA to secure transmissions.

## **Worm**

Adapted from *The Shockwave Rider*, a science fiction novel: an often malicious program that can copy and propagate itself over the Internet using email programs or other transport tools. May also compromise the security of an infected computer or cause system and data damage.

## **WPA**

Wi-Fi Protected Access: part of the 802.11 wireless standards, WPA is an extension and improvement of the WEP security protocol, offering better encryption and user authentication measures.

## **WPA2**

Part of the 802.11 wireless standards, WPA2 enhances the WPA security protocol. WEP, WPA, and WPA2 are all still in use, but WPA and WPA2 offer better protection.

## **XML**

Extensible Markup language: like HTML, a language Web programmers use to format and present information on the Web. Unlike HTML, it does not have a fixed set of formatting tags; rather, it is a meta-language that gives programmers the flexibility to create their own markup tags and thereby organize and present information in innovative ways.

## **802.11 or IEEE 802.11x**

A conventional set of standards for wireless network communication. There are several versions, or modulations, of 802.11. 802.11b and 802.11g are among the most popular. The 802.11 standards also define security protocols, including WEP, WPA, and WPA2.

### **Source:**

[http://www.symantec.com/norton/products/library/article.jsp?aid=security\\_glossary](http://www.symantec.com/norton/products/library/article.jsp?aid=security_glossary)